REMARKS

This Reply is responsive to the final Office Action[1] having a mailing date of March 22, 2007. Claims 1-6 and 8-22 were presented for examination in a second Request for Continued Examination and were rejected.

Claims 1-6 and 8-22 are rejected under 35 U.S.C. § 103(a) as being un-patentable over Sudia et al. (U.S. Patent No. 5,825,880; hereinafter "Sudia") and further in view of Boebert et al. (U.S. Patent No. 5,596,718, hereinafter "Boebert"). The rejection is respectfully traversed for at least the following reasons.

The Examiner appears to have taken conflicting positions during the course of this prosecution with regard to what is allegedly the equivalent of Applicants' claimed "node." For example, in the office action of May 4, 2006, on page 8, the Examiner says:

> **"Applicant's node is referred in Sudia as the trusted device or known as a smart card or the signing device. This trusted device comprises a microchip that has a microcontroller for executing programs and a crypto-unit that performs encryption/decryption and signature processes (col. 8, line 63-col. 9, line 23). Therefore, Sudia does teach executing the application program and cryptographic processing within the node."** (bold emphasis in the original)

THE SMART CARD IS APPLICANTS' NODE:

Very clearly, this says that it is the Examiner's position that Sudia allegedly shows Applicant's node as a "smart card." The passage cited (col. 8, line 63 - col. 9, line 23) is describing operation of the smart card shown in Fig. 3 of Sudia. For example, the beginning of that passage says:

> "Fig. 3 also illustrates a preferred architecture for a possible trusted device to be used by an authorizing agent. It comprises a single micro-chip encased on a card in a configuration known as a 'smart card'." (Sudia, col. 8, lines 62-65)

[1] The Office Action may contain a number of statements characterizing the cited references and/or the claims which Applicants may not expressly identify herein. Regardless of whether or not any such statement is identified herein, Applicants do not automatically subscribe to, or acquiesce in, any such statement.

Fig. 3 shows smart card 55 which operates in smart card reader 53 which, in turn, operates with workstation terminal 51. The passage further says:

> "The micro-chip may also include an optional 'crypto-unit' 46, which is a special purpose arithmetic accelerator unit having hardware for performing accelerated exponentiation and other arithmetic operation of encryption/decryption and signature processes." (Sudia, col. 9, lines 8-13)

Crypto unit 46 is also shown in Fig. 3 as being included on smart card 55. In addition, the smart card including its crypto unit is secure, at least to the extent that it is described as being tamper resistant. For example:

> "Each signing device, and each authorizing agents' smart card is assumed to be a 'trusted device' in that it is a *tamper-resistant device* that functions only in accord with stated characteristics, and whose manufacturer has endowed it with a device signature key pair and a device encryption key pair stored in a protected memory. At a minimum, the manufacturer of such a device will attest that the device will not divulge either its own or its user's private key(s) without an expensive tampering effort." (Sudia, col. 9, lines 41-49, emphasis added)

Each authorizing agents' smart card is a trusted device. As the above-quoted sections of Sudia clearly show, its smart card is tamper resistant and contains cryptographic functionality. It operates within a terminal, such as personal computer 51. Although personal computer 51 may be operating within a corporate environment that is otherwise unsecured, the tamper resistance of the smart card creates a secure terminal, or secure network node environment, at least to some extent. This cannot be ignored. Regardless, as the above quoted section from the May 4, 2006 office action shows, the Examiner's position had been that the smart card was equivalent to Applicant's claimed node.

THE SMART CARD IS NOT APPLICANTS' NODE:

In the final Office Action of March 22, 2007, the Examiner appears to both affirm this prior position that the smart card is Applicants' node and then challenge it in the same paragraph. On page 19 of the final Office Action it says: *"Thus, each smart card for use with each*

workstation or desktop reads on the claimed 'the node'." (emphasis added) This somewhat affirms the prior position. Clearly, this means that the Examiner is now reading the workstation with its smart card on Applicants' claimed node, somewhat consistent with the previous position taken in the May 4, 2006 office action described above where the smart card was considered as the node equivalent.

But, by curious contrast, at the end of that paragraph it says: "Therefore, the smart card or signing device is not being referred as a node or vault or message server." This seems to directly contradict the May 4, 2006 office action position that Sudia's smart card can be viewed as Applicants' node. Applicants do not fully understand the meaning of this statement and are confused by this seemingly contradictory position. Is the Examiner saying that the smart card, by itself, without card reader and terminal, is not a node-equivalent? If that is the meaning intended, then one could reason that the smart card does needs its reader for it to be functional, as well as its associated workstation, where all of that combined could be viewed as a node.

In any event, whether the Examiner's position is that the node is the smart card by itself or only after it is inserted into its reader in the workstation, what Applicants do understand is that the smart card in Sudia is tamper resistant as pointed-out in the quotation above (col. 9, lines 41-49). This protection can not be discounted or ignored. Tamper-resistance offers a certain level of security to the cryptographic functionality on the smart card, and to the network environment in which the cryptographic functionality is employed, whether one wishes it to be there or not. It is there. When the tamperproof smart card is inserted into its reader in the workstation, the smart card-workstation combination (node) takes on a degree of security based on the tamperproof aspect of the smart card.

Accordingly, this particular view of this "node" structure in Sudia necessarily prevents Sudia from reading on the node in Applicant's claims, because all of Applicant's claims recite a node, or a node in a network environment, that is not secure. For example, consider the language: "executing an application program at the node which is not secured" as recited in claim 1. As submitted many times in this prosecution, Applicants' nodes are not secure, but the Examiner's interpretation of a node in Sudia presents an inherently secure node- or at least nodes which are more secure than "not secure" as recited in Applicants' claims. Applicants submit that this is a sufficient difference to achieve allowability of these claims.

On page 4 of the final Office Action, in reference to a workstation with a smart card, it says that "This reads on the claimed the node is not secured and processing by a cryptographic processing component within the node." Applicants disagree, because there IS security inherent in the workstation-smart card combination; namely, the smart card is tamper proof or tamper resistant and that IS security, and particularly so, as it protects the cryptographic functionality of Sudia. Therefore, the Examiner cannot say that (1) Sudia's node is its workstation with its smart card and (2) that node is not secured, because it is secured to the extent of its smart card being tamper resistant.

In view of the above, Sudia does not disclose or suggest "executing an application program at the node which is not secured" as recited in claim 1, the unsecured node aspect of which appears in one form or another in all independent claims in this application.

Accordingly, the 35 U.S.C. § 103(a) rejection of the pending independent claims 1, 5, 9, 14, and 22 should be withdrawn and the claims allowed.

The dependent claims 2-4, 6, 8, 10-12 and 15-21 are likewise allowable, at least for reasons based on their dependencies from allowable base claims.

CONCLUSION

In view of the foregoing remarks, submitted after final rejection under rule 116, reconsideration and allowance are respectfully requested.

To the extent necessary, a petition for an extension of time under 37 C.F.R. § 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 07-2347 and please credit any excess fees to such deposit account.

Respectfully submitted,

By: /Eden Stright/ Eden Stright, Reg. 51,205, for
Joel Wall
Reg. No. 25,648

Date: May 21, 2007

Verizon
Patent Management Group
1515 Courthouse Road, Suite 500
Arlington, VA 22201-2909
Tel: 703.351.3586
CUSTOMER NO. 25537